(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 103 27 291 B4** 2005.03.24

(12) **Patentschrift**

(21) Aktenzeichen: **103 27 291.7**
(22) Anmeldetag: **17.06.2003**
(43) Offenlegungstag: **17.02.2005**
(45) Veröffentlichungstag der Patenterteilung: **24.03.2005**

(51) Int Cl.[7]: **H04L 12/22**
H04L 9/00

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden.

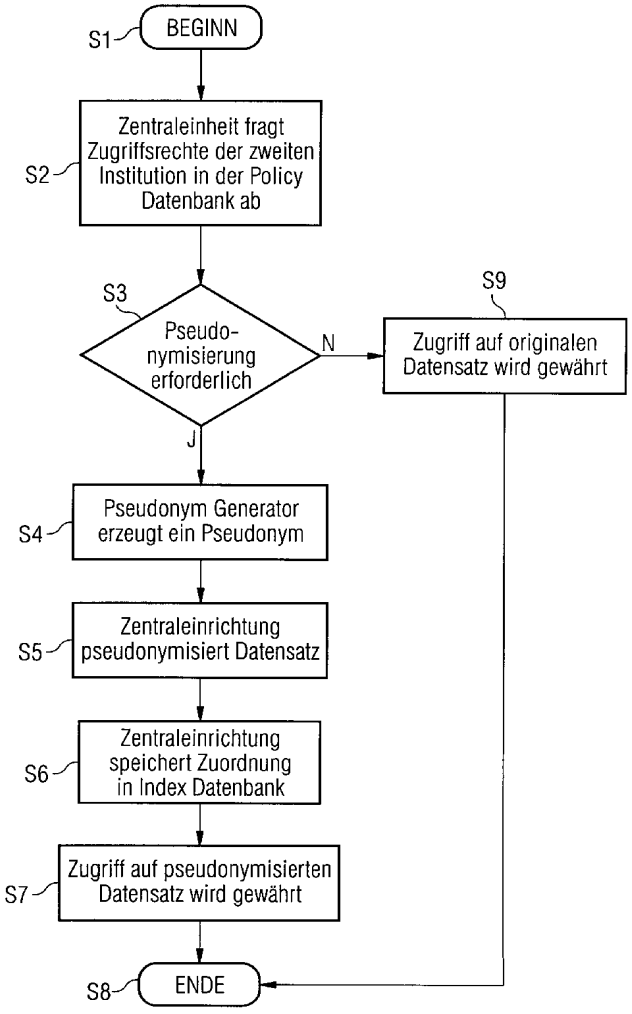
(71) Patentinhaber:
Siemens AG, 80333 München, DE

(72) Erfinder:
Christ, Tilo, 91058 Erlangen, DE; Schmidt, Volker, Dr., 91054 Erlangen, DE; Schüll, Hans-Dieter, 91085 Weisendorf, DE; Striebel, Werner, 90592 Schwarzenbruck, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 102 53 676 A1
WO 02/0 80 547 A1

(54) Bezeichnung: **System zur Wahrung der Vertraulichkeit von elektronischen Daten in einem Netzwerk**

(57) Hauptanspruch: System zur Wahrung der Vertraulichkeit von elektronischen Daten in einem Netzwerk mit
einem Pseudonym Generator (9) zur Erstellung von Pseudonymen in Abhängigkeit von durch eine erste Institution (1a, 1b ... 1n) zur Verfügung gestellten Daten,
einer Policy Datenbank (8) zur Speicherung von Pseudonymisierungsvorschriften für Daten, die durch die erste Institution (1a, 1b ... 1n) über das Netzwerk für eine zweite Institution (1, 1b, ... 1n) zur Verfügung gestellt werden sollen und
einer Zentraleinheit (4) zur Annahme einer Datenanfrage der zweiten Institution (1a, 1b, ... 1n) und Steuerung der Pseudonymisierung der angeforderten Daten entsprechend den in der Policy Datenbank (8) gespeicherten Pseudonymisierungsvorschriften,
dadurch gekennzeichnet,
dass die Zentraleinheit (4) jedem Datensatz einmalig einen Satz an Pseudonymen zuordnet und bei jeder Datenanfrage der zweiten Institution (1a, 1b ... 1n) den einmalig zugeordneten Satz an Pseudonymen verwendet.



Beschreibung

[0001] Die Erfindung betrifft ein System zur Wahrung der Vertraulichkeit von elektronischen Daten in einem Netzwerk gemäß dem Patentanspruch 1.

[0002] Bei der Übermittlung von vertraulichen Daten oder bei dem Zugriff auf vertrauliche Daten ist es besonders im Falle von medizinischen Daten nötig, diese ganz oder teilweise zu verschlüsseln, insbesondere z.B. den Namen des Patienten, des behandelnden Arztes oder der Arztpraxis.

Stand der Technik

[0003] Ein Anonymitätssystem zur Verschlüsselung von Daten ist in der Patentschrift US 6,389,533 B1 offenbart. Hierbei wird in einem Anonymitätssytem, falls auf eine einkommende Nachricht eine Antwort erwünscht ist, vor der Weiterleitung der Nachricht der Sender verschlüsselt und die Nachricht anschließend an den Empfänger oder erst an weitere Anonymitätssysteme und dann an den Empfänger geschickt. So ist es zum einen möglich, zu verhindern, dass der Empfänger die wahre Identität des Senders kennt. Zum anderen kann aber, wenn der Empfänger eine Antwort schickt, diese nach einer Entschlüsselung des Senders durch das Anonymitätssystem an den Sender weitergeleitet werden.

[0004] Nachteilig hierbei ist jedoch, dass die Daten nur einmal über mittelt werden und nicht beispielsweise über ein Netzwerk dauerhaft zur Verfügung gestellt werden.

[0005] Die Offenlegungsschrift DE 102 53 676 A1 offenbart ein Verfahren für die Fernübertragung und/oder Betrachtung sensibler Daten eines Anwendungs-Rechners. Hierbei erfolgt die Fernübertragung und/oder Betrachtung der sensiblen Daten auf Anforderung. Vor der Fernübertragung und/oder Betrachtung werden geheimhaltungsbedürftige Datenbestandteile der angeforderten Daten, z. B. Daten zur Identifizierung von Personen, identifiziert und durch ein Datenschutz-Modul eliminiert.

[0006] Die Druckschrift WO 02/080457 A1 offenbart ein System zum Verarbeiten von Datenanfragen von Clients über ein Netzwerk. Das System umfasst hierbei einen Anwendungsserver, der an das Netzwerk angebunden ist und eine semantische Firewall zum Übermitteln und Filtern der Dateninhalte zwischen dem Anwendungsserver und den Clients. Der Anwendungsserver stellt hierbei Dateninhalte von einer Datenbasis den Clients über das Netzwerk bereit und die semantische Firewall beschränkt den Zugriff auf einen Teil des Dateninhalts für einen oder mehr Clients.

Aufgabenstellung

[0007] Aufgabe der vorliegenden Erfindung ist es deshalb, in einem Netzwerk von Teilnehmern mit unterschiedlichen Teilaufgaben Daten über ein zentrales System so zur Verfügung zu stellen, dass die Vertraulichkeit der Daten gewahrt wird, ohne dabei die Arbeitsprozesse zu behindern.

[0008] Die Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 gekennzeichneten Merkmale gelöst.

[0009] Vorteilhafterweise verfügt das System über eine Patienten Index Datenbank zur Verwaltung von patientenidentifizierenden Daten.

[0010] Das System verfügt zweckmäßigerweise über eine Institutionen Index Datenbank zur Verwaltung von institutionsidentifizierenden Daten.

[0011] Vorzugsweise verfügt das System über eine Personen Index Datenbank zur Verwaltung von Daten, die sich auf Personen beziehen, welche innerhalb der Institutionen arbeiten.

[0012] In einer bevorzugten Ausführungsform erzeugt der Pseudonym Generator Pseudonyme für Patientennamen, Institutionen und in den Institutionen arbeitenden Personen.

[0013] Zweckmäßigerweise speichert die Zentraleinheit die Zuordnung des erzeugten Pseudonyms zu dem von der ersten Institution genannten Patientennamen in der Patienten Index Datenbank.

[0014] Vorteilhafterweise speichert die Zentraleinheit die Zuordnung des erzeugten Pseudonyms zu einer Institution in der Institutionen Index Datenbank.

[0015] Vorzugsweise speichert die Zentraleinheit die Zuordnung des erzeugten Pseudonyms zu einer in einer Institution arbeitenden Person in der Personen Index Datenbank.

Ausführungsbeispiel

[0016] Ausführungsbeispiele der Erfindung werden im folgenden anhand von Figuren näher erläutert. Dabei zeigen

[0017] **Fig.** 1 eine schematische Darstellung eines Systems zur Wahrung der Vertraulichkeit von elektronischen Daten und

[0018] **Fig.** 2 ein Flussdiagram der in dem System ablaufenden Schritte.

[0019] **Fig.** 1 zeigt eine schematische Darstellung eines Systems zur Wahrung der Vertraulichkeit von

elektronischen Daten. Institutionen **1a**, **1b**, ... **1n** sind hierbei über eine Kommunikationseinrichtung **2** mit dem System **3** verbunden. Bei den Institutionen **1a**, **1b**, ... **1n** handelt es sich beispielsweise um Arztpraxen, Kliniken, Forschungseinrichtungen, medizinische Geräte mit Datenschnittstelle, Qualitätssicherungsstellen oder Patienten, die auf einem gemeinsamen Datenpool zugreifen oder den Pseudonymisierungsservice nutzen. Die Institutionen **1a**, **1b** ... **1n** sind mit dem System **3** über eine Kommunikationseinrichtung **2** verbunden, welche ein Netzwerk, beispielsweise ein Netzwerk über das Internet oder ein geschlossenes Netzwerk sein kann.

[0020] Das System **3** verfügt über einen Pseudonym Generator **9**, welcher Pseudonyme erstellt, die bei der Übermittlung von Daten oder bei dem Zugriff auf Daten anstelle derjenigen Daten eingesetzt werden, die nicht übermittelt werden sollen, beispielsweise Patientennamen, Arztpraxen oder Ärzte.

[0021] In einer Patienten Index Datenbank **5** werden die Zuordnungen zwischen einem bestimmten Patienten und den entsprechenden für die einzelnen Institutionen **1a**, **1b** ... **1n** geltenden Pseudonymen gespeichert, d.h. es wird gespeichert, für welchen originalen Patientennamen welches Pseudonym eingesetzt wurde. Analog werden in einer Institutionen Index Datenbank **6** und in einer Personen Index Datenbank **7** die Zuordnungen zwischen den Institutionen **1a**, **1b**, ... **1n** und den Pseudonymen sowie die Zuordnungen zwischen den Institutionen arbeitenden Personen und den entsprechenden Pseudonymen gespeichert.

[0022] In einer Policy Datenbank **8** sind die Zugriffsrechte für die einzelnen Institutionen **1a**, **1b**, ... **1n** gespeichert, d.h. welche Daten pseudonymisiert werden müssen, wenn eine bestimmte Institution auf die Daten zugreift, und welcher Art die Pseudonymisierung zu sein hat, z.B. Löschung oder Anonymisierung.

[0023] Eine Zentraleinheit **4** in dem System **3** übernimmt die Aufgabe der Annahme von Datenanfragen durch eine Institution **1a**, **1b**, ... **1n**, der Pseudonymisierung der Daten entsprechend der Zugriffsrechte der anfragenden Institutionen, der Speicherung der Zuordnung zwischen den originalen Daten und dem jeweiligen Pseudonym in der entsprechenden Index Datenbank und der Übermittlung bzw. des Gewährens der Zugriffsrechte auf die angeforderten pseudonymisierten Daten.

[0024] Das System **3** verwaltet somit für jede teilnehmende Institution **1a**, **1b**, ... **1n** die für diese Institution geltenden Pseudonyme. Sobald Daten an eine Institution gesandt werden oder von dieser eingesehen werden, entscheidet das System **3** anhand der in der Policy Datenbank **8** gespeicherten Zugriffsrechte, welche Daten diese Institution im Klartext sehen darf, und welche Daten verborgen werden müssen. Den Zugriffsrechten entsprechend werden die Daten für den Teilnehmer modifiziert.

[0025] Daten können beispielsweise medizinische Daten eines Patienten sein, die in einem Datenpool verwaltet werden, oder Röntgenbilder, Protokolle von medizinischen Geräten (MR, CT), die Patientendaten beinhalten.

[0026] Um die Personen- und institutionsidentifizierenden Daten der Teilnehmer voreinander zu verbergen, ohne dass die Arbeitsprozesse behindert werden, werden die Daten auf unterschiedliche Art modifiziert. Vom System **3** werden verschiedene Pseudonymisierungsstufen unterstützt: Dies umfasst, namenverändernde, teilpseudonyme und offene Arbeitsabläufe.

[0027] Eine Möglichkeit ist die Übermittlung namenveränderter Daten, d.h. dass die eingestellten Daten berechtigten Stellen eine Auflösung des Pseudonyms und damit die Rückverfolgung der erstellenden Institution/Person und/oder des Patienten zulassen. In diesem Falle wird für denselben Patienten somit immer dasselbe Pseudonym verwendet, die entsprechende Zuordnung zwischen Patient und Pseudonym wird in der Patienten Index Datenbank **5** gespeichert, auf welche nur die Zentraleinheit **4** Zugriff hat.

[0028] Des Weiteren besteht die Möglichkeit, die Daten teilpseudonym zu übermitteln, wodurch nur Teile der identifizierenden Daten pseudonymisiert sind. Darüber hinaus unterstützt das System völlig offene Arbeitsläufe, bei welchen die Daten ohne Modifikation übermittelt werden. Das Pseudonym entspricht somit den tatsächlichen originalen Daten.

[0029] Darüber hinaus wird durch das System **3** zusätzlich eine Identifikation der geschützten Daten verhindert, indem gegenüber jeder Stelle die Daten unterschiedlich pseudonymisiert werden können. Damit entfällt die Möglichkeit für Teilnehmer, unter Umgehung des Systems über ein gemeinsames bekanntes Pseudonym die Zuordnung zu einem Patienten, einer Institution oder einer Person wieder herstellen zu können.

[0030] In **Fig.** 2 ist der Ablauf der einzelnen Schritte bei der Übermittlung oder Gewährung von Zugriffsrechten auf Daten in einem Flußdiagramm dargestellt. In einem Schritt S1 beginnt der Ablauf, beispielsweise durch die Anfrage einer zweiten Institution **1a**, **1b**, ... **1n**, welche auf Daten einer ersten Institution **1a**, **1b**, ... **1n** zugreifen möchte. Im Schritt S2 fragt die Zentraleinheit **4** die Zugriffsrechte der anfragenden zweiten Institution in der Policy Datenbank **8** ab.

[0031] In einem dritten Schritt S3 wird überprüft, ob für die Datenübermittlung zur zweiten Institution von der ersten Institution eine Pseudonymisierung erforderlich ist. Falls nicht, wird in einem Schritt S9 der zweiten Institution der Zugriff auf die originalen, nicht modifizierten Daten gewährt. Falls hingegen eine Pseudonymisierung erforderlich ist, veranlasst in einem Schritt S4 die Zentraleinheit den Pseudonym Generator, ein Pseudonym zu erzeugen, und pseudonymisiert in einem Schritt S5 die Daten entsprechend der in der Policy Datenbank gespeicherten Zugriffsrechte.

[0032] In einem Schritt S6 speichert die Zentraleinrichtung **4** die eben erstellte Zuordnung der originalen Daten und des Pseudonyms in der entsprechenden Indexdatenbank. Falls beispielsweise für Patientennahmen Pseudonyme erstellt wurden, so speichert die Zentraleinheit **4** die entsprechende Zuordnung in der Patientendatenbank **5**.

[0033] In einem Schritt S7 wird nun der zweiten anfragenden Institution **1a**, **1b**, ... **1n** der Zugriff auf die pseudonymisierten Daten gewährt. In einem Schritt S8 endet der Prozess.

[0034] Im Folgenden wird anhand verschiedener Beispiele die Arbeitsweise des Systems **3** verdeutlicht.

[0035] Im Fallbeispiel **1** legt ein Arzt eine Patientenakte an, eine qualitätssichernde Institution (Q-Institution) greift auf die medizinischen Daten zu, wertet diese aus und gibt dem Arzt ein Feedback, ohne die Arzt/Patientenidentität zu kennen.

[0036] Der Ablauf im Detail gestaltet sich folgendermaßen: Der Arzt legt in einer Institution **1a**, **1b**, ... **1n** eine neue Patientenakte für einen seiner Patienten an. Durch die Kommunikationseinrichtung **2** ist diese erste Institution mit dem System **3** verbunden. Nach Anlegen der neuen Patientenakte vergibt die Zentraleinheit **4** für den Patienten einen internen, d.h. im System **3** geltenden Index und speichert diesen in der Patienten Index Datenbank **5**.

[0037] Erfolgt nun eine Anfrage einer qualitätssichernden Institution, so weist die Zentraleinheit **4** aufgrund der in der Policy Datenbank **8** gespeicherten Zugriffsrechte, dass die Q-Institution Zugriff auf Teile der medizinischen Daten der ersten Institution hat, aber weder die wahre Patientenidentität noch die Identität des Arztes oder der Arztpraxis erfahren darf. Der Pseudonym Generator erzeugt somit Pseudonyme für den Arzt, die Arztpraxis und den Patienten und die Zentraleinheit setzt diese anstelle der tatsächlichen Namen des Arztes, der Arztpraxis und des Patienten ein.

[0038] Greift nun die Q-Institution auf die Daten zu, so sind die oben genannten identifizierenden Daten durch für die Q-Institutionen generierten Pseudonyme ersetzt. Die Zuordnung zwischen den identifizierenden Daten und den von dem Pseudonym Generator **9** identifizierten Pseudonymen werden von der Zentraleinheit in der Patienten Index Datenbank **5**, in der Institutionen Index Datenbank **6** und in der Personen Index Datenbank **7** gespeichert.

[0039] Nach Auswertung der Daten erzeugt die Q-Institution eine Antwort, die einen bestimmten Teilnehmer, welcher der Q-Institution unbekannt ist, zugeordnet werden soll. Dafür setzt die Q-Institution die ihr bekannten Pseudonymen ein und sendet die Daten an das System **3**. Die Zentraleinheit **4** in dem System **3** identifiziert als sendende Stelle die Q-Institution, löst darüber die Pseudonyme auf und führt die gewünschte Operation aus, beispielsweise eine Nachricht an den Arzt, ein Speichern in der Patientenakte oder Nachricht an andere Teilnehmer.

[0040] Der Arzt selbst kann Pseudonyme für seine Patienten vergeben. In diesem Falle kennt das System **3** die wahre Identität des Patienten nicht. Wenn es somit mit dem Arzt kommuniziert, dann verwendet es das vom Arzt für den Patienten vergebene Pseudonym.

[0041] Ein weiteres Fallbeispiel ist das einer möglichen Fernwartung von medizinischen Geräten. In einer medizinischen Institution **1a**, **1b**, ... **1n**, beispielsweise in einem Krankenhaus oder einer Praxis, stehen medizinische Geräte wie z.B. MR, CT, Röntgen, Angiografiegeräte, Ultraschall, PET, Beatmungsgeräte oder Infusionsgeräte. Diese sollen nun von einem Service oder Ingenieur per Fernwartung oder Fernzugriff bedient werden, ohne dass dabei der Service Ingenieur die Patientendaten, die Arztdaten oder die Institutionsdaten kennt.

[0042] In diesem Beispiel pseudonymisiert das System **3** die aus dem Kliniksystem bzw. aus dem Gerät kommenden Daten, um eine Identifikation des Patienten oder einer Institution zu verhindern, speichert diese entsprechende Zuordnung jedoch in der Datenbank. Wenn nun seitens des Service Ingenieurs Fehleranalysen zu der überprüften Institution übermittelt werden sollen, so ermöglicht die in der Index Datenbank gespeicherte Zuordnung dem System **3**, die Daten wieder an die Institution senden zu können, ohne dass der Service Ingenieur die tatsächliche Identität der Institution oder des Patienten kennen muss.

Patentansprüche

1. System zur Wahrung der Vertraulichkeit von elektronischen Daten in einem Netzwerk mit
einem Pseudonym Generator (**9**) zur Erstellung von Pseudonymen in Abhängigkeit von durch eine erste

Institution (**1a**, **1b** ... **1n**) zur Verfügung gestellten Daten,
einer Policy Datenbank (**8**) zur Speicherung von Pseudonymisierungsvorschriften für Daten, die durch die erste Institution (**1a**, **1b** ... **1n**) über das Netzwerk für eine zweite Institution (**1**, **1b**, ... **1n**) zur Verfügung gestellt werden sollen und
einer Zentraleinheit (**4**) zur Annahme einer Datenanfrage der zweiten Institution (**1a**, **1b**, ... **1n**) und Steuerung der Pseudonymisierung der angeforderten Daten entsprechend den in der Policy Datenbank (**8**) gespeicherten Pseudonymisierungsvorschriften,
dadurch gekennzeichnet,
dass die Zentraleinheit (**4**) jedem Datensatz einmalig einen Satz an Pseudonymen zuordnet und bei jeder Datenanfrage der zweiten Institution (**1a**, **1b** ... **1n**) den einmalig zugeordneten Satz an Pseudonymen verwendet.

2. System nach Anspruch 1, gekennzeichnet durch eine Patienten Index Datenbank (**5**) zur Verwaltung von patientenidentifizierenden Daten.

3. System nach einem der vorhergehenden Ansprüche, gekennzeichnet durch eine Institutionen Index Datenbank (**6**) zur Verwaltung von institutionsidentifizierenden Daten.

4. System nach einem der vorhergehenden Ansprüche, gekennzeichnet durch eine Personen Index Datenbank (**7**) zur Verwaltung von Daten, die sich auf Personen beziehen, welche innerhalb der Institutionen (**1a**, **1b**, ... **1n**) arbeiten.

5. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Pseudonym Generator (**9**) Pseudonyme für Patientennamen, Institutionen (**1a**, **1b**, ... **1n**) und in den Institutionen arbeitende Personen erzeugt.

6. System nach Anspruch 5, dadurch gekennzeichnet, dass die Zentraleinheit (**4**) die Zuordnung des erzeugten Pseudonyms zu dem von der ersten Institution (**1a**, **1b**, ... **1n**) genannten Patientennamen in der Patienten Index Datenbank (**5**) speichert.

7. System nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, dass die Zentraleinheit (**4**) die Zuordnung des erzeugten Pseudonyms zu einer Institution (**1a**, **1b**, ... **1n**) in der Institutionen Index Datenbank (**6**) speichert.

8. System nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass die Zentraleinheit (**4**) die Zuordnung des erzeugten Pseudonyms zu einer in einer Institution (**1a**, **1b**, ... **1n**) arbeitenden Person in der Personen Index Datenbank (**7**) speichert.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

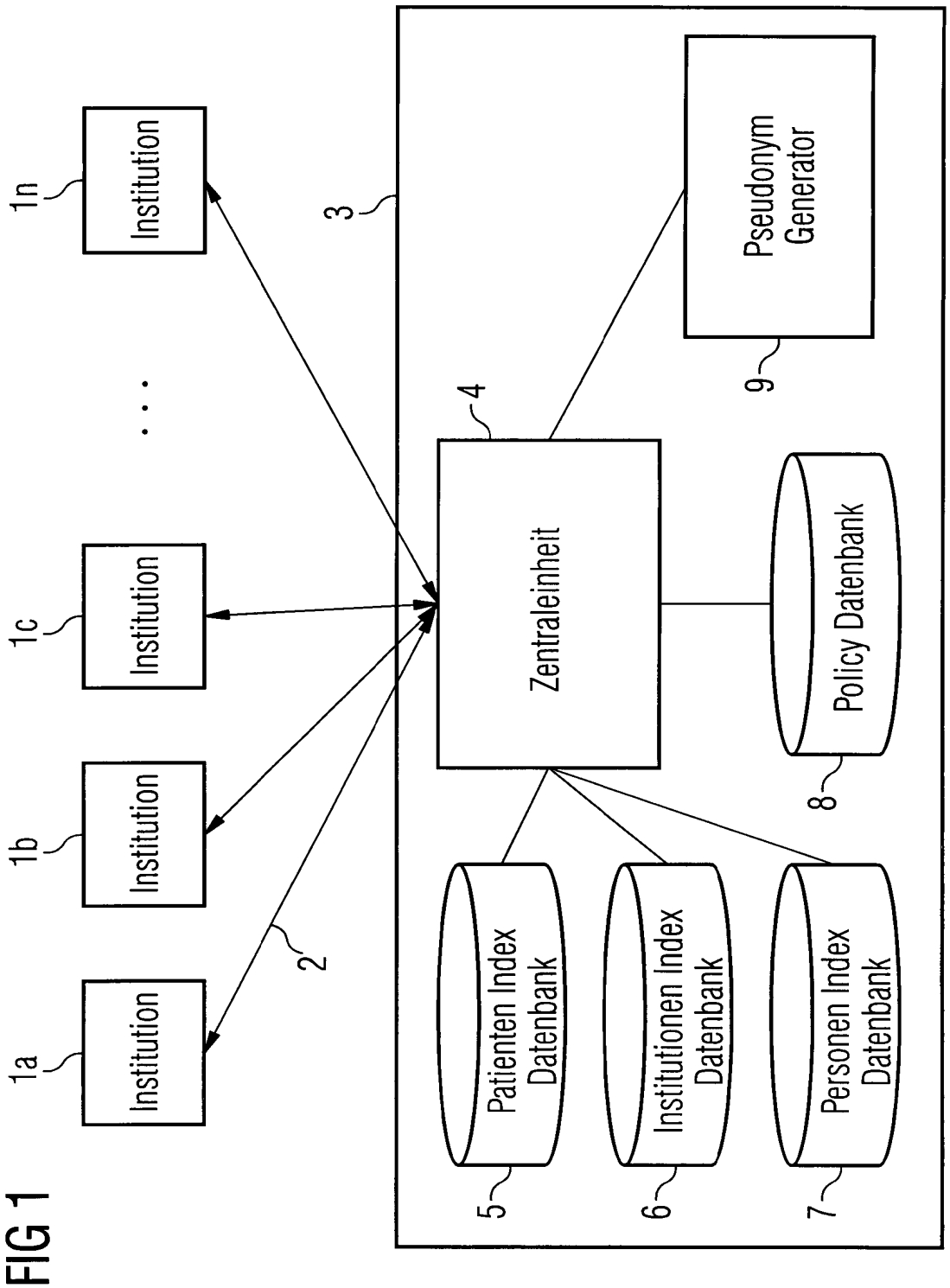
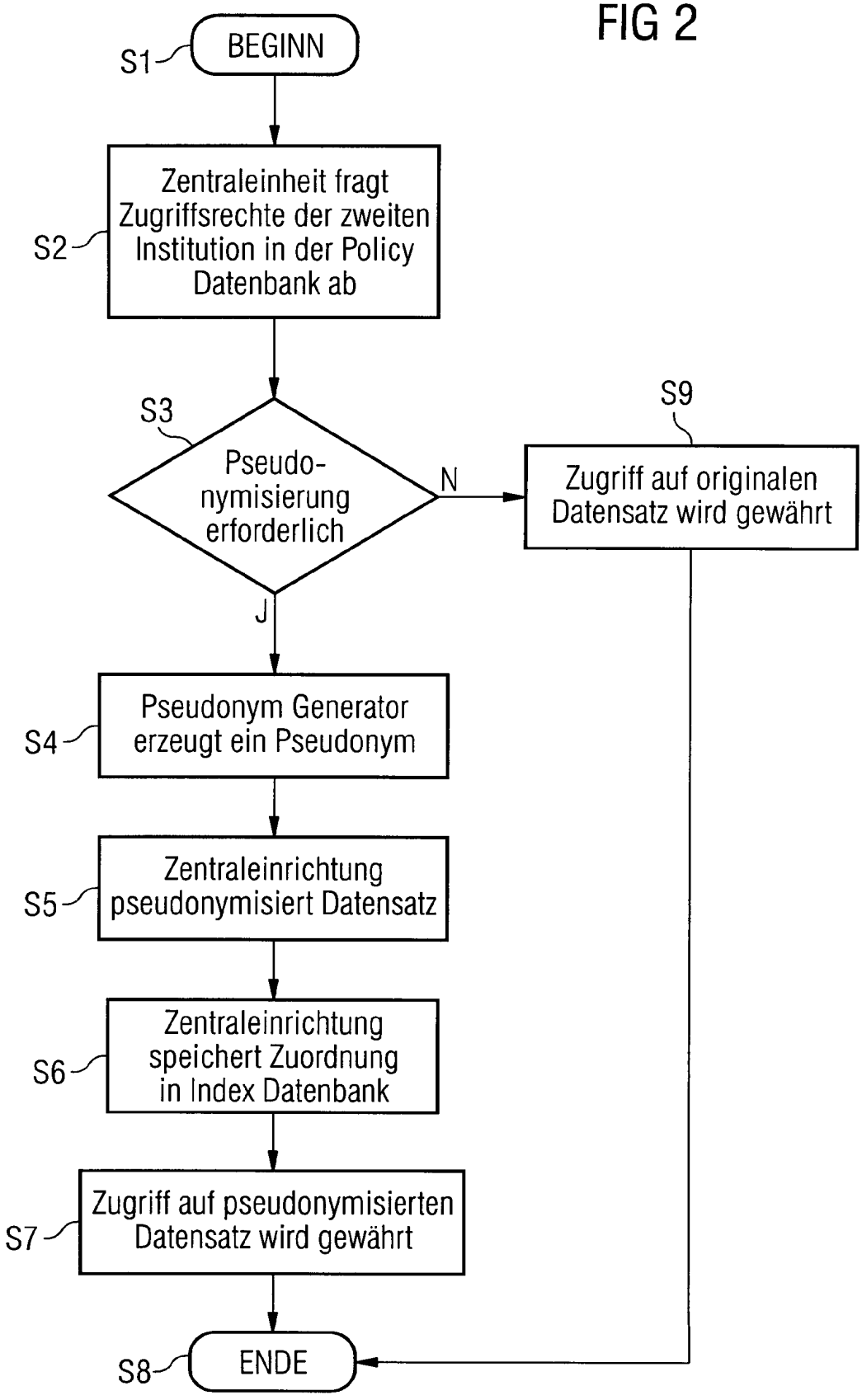


FIG 1

FIG 2


S1
BEGINN
S2
Zentraleinheit fragt Zugriffsrechte der zweiten Institution in der Policy Datenbank ab
S3
Pseudo-nymisierung erforderlich
N
S9
Zugriff auf originalen Datensatz wird gewährt
J
S4
Pseudonym Generator erzeugt ein Pseudonym
S5
Zentraleinrichtung pseudonymisiert Datensatz
S6
Zentraleinrichtung speichert Zuordnung in Index Datenbank
S7
Zugriff auf pseudonymisierten Datensatz wird gewährt
S8
ENDE

[0001] The invention concerns a system for the keeping of the privacy of electronic data in a network in accordance with the patent claim 1.

[0002] During the transmission of confidential data or with the access to confidential data it is particularly necessary in case of of medical data to code these totally or partly in particular e.g. the names of the patient, the treating physician or the medical practice.

State of the art

[0003] An anonymity system for the coding of data is revealed in the patent specification US 6 389 533 B1. Here in a Anonymitätssytem if on a coming in message an answer is desired, before the forwarding of the message of the transmitters coded and the message afterwards to the receiver or only to further anonymity systems and then to the receiver skillfully. Like that it is on the one hand possible to prevent that the receiver knows the true identity of the transmitter. On the other hand however, if the receiver sends an answer, this can be passed on after a decoding of the transmitter by the anonymity system to the transmitter.

[0004] Unfavorably here it is however that the data are only once conveyed and not for example over a network durably are made available. The moreover one the same kind of the coding always takes place, and it is not differentiated, how confidential the data are or whether certain receivers may know the true identity of the transmitter or or see other data unencrypted.

Setting of tasks

[0005] Task of the available invention is it therefore to make available in a network of participants with different subtasks data over a central system in such a way the fact that on one ?need tons know? - basis only the data is available, which by the individual participant for the solution of its subtask are needed, and that the privacy of the data is protected, without in it the working processes to obstruct.

6/17/03

[0006] The task is solved according to invention by the characteristics marked in the patent claim 1.

[0007] In accordance with the available invention a system to the keeping of the privacy described by electronic data in a network with an alias generator to the production by aliases as a function of data provided by a first institution, a Policy data base to storage by Pseudonymisierungsvorschriften for data, those by the first institution over the network for a second institution to be made available to be supposed and a central processing unit to the acceptance of a data inquiry of the second institution and controlling of the Pseudonymisierung according to of the requested data in the Policy data base stored Pseudonymisierungs regulations.

[0008] By the use of a network is possible the constant access to the data provided in the network by the institutions attached to the network. Beyond that make possible in the Policy data base stored Pseudonymisierungs regulations a flexible Pseudonymisierungs concept, since depending upon access authorization of the second institution the data are differently pseudonymisiert and so different stages of the Pseudonymisierung to be achieved to be able.

[0009] Favourable way has the system patients index data base for the administration of patient-identifying data.

[0010] The system has appropriately institutions index data base for the administration of institution-identifying data.

[0011] Preferably the system has persons index data base for the administration of data, which refer to persons, who work within the institutions.

[0012] In a preferential execution form the aliases generator of aliases for patient name, institutions and in the institutions produces working persons.

[0013] The central processing unit appropriately stores the allocation of the produced alias to the patient name in the patients index data base, specified by the first institution.

[0014] Favourable way stores the central processing unit the allocation of the produced alias to an institution in the institutions index data base.
[0015] Preferably the central processing unit stores the allocation of the produced alias to a person in the persons index data base, working in an institution.

Remark example

[0016] Remark examples of the invention are more near described in the following on the basis figures. Show
[0017] Fig. 1 a schematic representation of a system for the keeping of the privacy of electronic data and
[0018] Fig. 2 a flow chart of the steps running off in the system.
[0019] Fig. 1 points a schematic representation of a system to the keeping of the privacy of electronic data. Institutions 1a, 1b,? 1n are here connected by a communication device 2 with the system 3. With the institutions 1a, 1b,? 1n concerns it for example medical practices, hospitals, research establishments, medical instruments with data interface, quality assurance places or patients, which access on a common data pool or which Pseudonymisierungsservice use. The institutions 1a, 1b? 1n are connected with the system 3 by a communication device 2, which can be a network, for example a network over Internet or a closed network.
[0020] The system 3 has alias a generator 9, which provides aliases, which are used during the transmission by data or with the access to data in place of those data, which are not to be conveyed, for example patient names, medical practices or physicians.
[0021] In patients index data base 5 are stored the allocations between a certain patient and the appropriate for the individual institutions 1a, 1b? 1n valid aliases, i.e. it is stored, for which original patient names which alias was used. Institutions become similar index data base 6 and in persons index data base 7 the allocations between the institutions 1a, 1b, in? 1n and the aliases

as well as the allocations between the institutions working persons and the appropriate aliases stored.

[0022] In a Policy data base 8 are the rights of access for the individual institutions 1a, 1b,? 1n stored, i.e. which data must be pseudonymisiert, if a certain institution accesses the data, and which kind the Pseudonymisierung has to be, e.g. Deletion or anonymization.

[0023] A central processing unit 4 in the system 3 takes over the task of the acceptance of data inquiries by an institution 1a, 1b,? 1n, the Pseudonymisierung according to data the rights of access of the inquiring institutions, the storage of the allocation between the original data and the respective alias in the appropriate index data base and the transmission and/or. granting the rights of access on the requested pseudonymisierten data.

[0024] The system 3 administers thus for each participating institution 1a, 1b,? 1n the aliases valid for this institution. As soon as data are sent to an institution or by this are seen, the system 3 decides 8 stored rights of access, which data this institution in the plain language may see on the basis in the Policy data base, and which data to be hidden to have. The data for the participant are modified accordingly to the rights of access.

[0025] Data can be for example medical data of a patient, which are administered in a data pool, or radiographs, minutes of medical instruments (MR, CT), which contain patient data.

[0026] In order to hide person and institution-identifying data of the participants before each other, without the working processes are obstructed, the data in different kind are modified. By the system 3 different Pseudonymisierungsstufen is supported: This covers anonymous and/or. name-hiding, name-changing, part aliases and open operational sequences.

[0027] Anonymous and/or. name-hiding it means here that the adjusted data permit no more backtracing concerning for example the providing institution, person and/or the patient. In this case for each new data inquiry a new alias

is thus created, whereby no allocation to same patients, institutions or persons is possible.

[0028] A further possibility is the transmission of name-changed data, i.e. that the adjusted data entitled places a dissolution of the alias and thus the backtracing of the providing institution/person and/or the patient permit. In this case for the same patient the same alias is thus always used, who appropriate allocation stored between patient and alias in the patients index data base 5, on which only the central processing unit has 4 access.

[0029] The moreover one the possibility exists of conveying the data part alias whereby only parts of the identifying data are pseudonymisiert. Beyond that the system supports completely open work runs, with which the data without modification are conveyed. The alias corresponds thus to the actual original data.

[0030] Beyond that by the system 3 additionally an identification of the protected data is prevented, as in relation to each place the data can be differently pseudonymisiert. Thus the possibility for participants is void of being able to repair under evasion of the system over a common well-known alias the allocation to a patient, an institution or a person.

[0031] In Fig. the expiration of the individual steps represented 2 during the transmission or grant of rights of access on data is in a flow chart. In a step S1 the expiration, for example by the inquiry of a second institution 1a, begins 1b,? 1n, which on data of a first institution 1a, 1b,? 1n to access would like. In the step S2 the central processing unit 4 queries the rights of access of the inquiring second institution in the Policy data base 8.

[0032] In a third step S3 it is examined whether for the data communication for the second institution of the first institution a Pseudonymisierung is necessary. Otherwise, in a step S9 of the second institution that is granted to access to the original, not modified data. If however a Pseudonymisierung is necessary, the central processing unit arranges the alias generator to produce an alias and pseudonymisiert in a step S5 according to data into the

Policy data base stored rights of access in a step S4.

[0033] In a step S6 the central mechanism 4 stores the evenly provided allocation of the original data and the alias in the appropriate index data base. If for example for patient-taken aliases were provided, then the central processing unit 4 stores the appropriate allocation in the patient data bank 5.

[0034] In a step S7 now the second inquiring institution 1a, 1b becomes,? 1n that access to the pseudonymisierten data grants. In a step S8 the process ends.

[0035] In the following on the basis different examples the function of the system 3 is clarified.

[0036] In the case example 1 a physician puts on a patient document, a quality-assurance institution (Q-institution) accesses the medical data, evaluates these and gives to the physician a feedback, without knowing the physician/patient identity.

[0037] The expiration in the detail turns out as follows: The physician puts 1a, in an institution 1b,? 1n a new patient document for one of its patients on. By the communication device 2 this first institution is connected with the system 3. In accordance with creation of the new patient document the central processing unit 4 for the patient assigns an internal, i.e. in the system 3 valid index and stores this in the patients index data base 5.

[0038] Taken place now an inquiry of a quality-assurance institution, then the central processing unit 4 points 8 stored rights of access due to in the Policy data base that the Q-institution has access to parts of the medical data of the first institution, but neither the true patient identity nor the identity of the physician or the medical practice experienced may. The aliases generator produced thus this uses aliases for the physician, the medical practice and the patient and the central processing unit in place of the actual names of the physician, the medical practice and the patient.

[0039] Now if the Q-institution accesses the data, then the identifying data specified above are through replaced for the Q-institutions of generated

aliases. The allocation between the identifying data and of the alias the generator 9 identified aliases are stored by the central processing unit in the patients index data base 5, in the institutions index data base 6 and in the persons index data base 7.

[0040] After evaluation of the data the Q-institution produces an answer, which a certain participant, which is unknown to the Q-institution, to be assigned is. But the Q-institution uses it well-known aliases and sends the data to the system 3. The central processing unit 4 in the system 3 identified as sending place the Q-institution, dissolves over it the aliases and implements the desired operation, for example a message to the physician, storing in the patient document or message to other participants.

[0041] The physician can assign aliases for its patients. In this case the system 3 does not know the true identity of the patient. If it communicates thus with the physician, then it uses the alias assigned by the physician for the patient.

[0042] If the system knows due to in the Policy data base 8 stored right of access that the Q-institution may see only anonymous data, then for each procedure between the system 3 and the Q-institution new aliases are used, whereby an allocation from data to certain patients, medical practices or physicians is not possible.

[0043] A further case example is that possible remote maintenance of medical instruments. In a medical institution 1a, 1b,? 1n, for example in a hospital or a practice, stand medical instruments like e.g. MR, CT, Roentgen, Angiografiegeräte, Ultraschall, PET, respirators or infusion devices. These are to be served now by a service or an engineer by remote maintenance or main line train reef, without with it the service engineer the patient data, which knows physician data or the institution data.

[0044] In this example the system 3 pseudonymisiert from the hospital system and/or. from the equipment, in order to prevent an identification of the patient or an institution, this appropriate allocation stores coming data however in the

data base. If now on the part of the service of engineer error analyses are to be conveyed to the examined institution, then into the index data base makes possible stored allocation for the system 3 to be able to send the data the institution without the service engineer must know the actual identity of the institution or the patient.

Europäisches Patentamt
European Patent Office
Office européen des brevets

Claims of DE10327291	Print	Copy	Contact Us	Close

Result Page

. System for the keeping of the privacy of electronic data in a network also
an alias generator (9) to the production of aliases as a function of by a first institution (1a, 1b? 1n) provided data,
a Policy data base (8) to the storage of Pseudonymisierungsvorschriften for data, those by the first institution (1a, 1b? 1n) over the network for a second institution (1, 1b,? 1n) to be made available are and
a central processing unit (4) to the acceptance of a data inquiry of the second institution (1a, 1b,? 1n) and controlling of the Pseudonymisierung according to of the requested data in the Policy data base (8) stored Pseudonymisierungsvorschriften.
2. System according to requirement 1, characterized by patients index data base (5) to the administration of patient-identifying data.
3. System after one of the preceding requirements, characterized by institutions index data base (6) to the administration of institution-identifying data.
4. System after one of the preceding requirements, characterized by persons index data base (7) to the administration of data, which refer to persons, who within the institutions (1a, 1b,? 1n) work.
5. System after one of the preceding requirements, by the fact characterized that the aliases generator (of 9) aliases for patient name, institutions (1a, 1b,? 1n) and in the institutions working persons produces.
6. System according to requirement 5, by the fact characterized that the central processing unit (4) stores the allocation of the produced alias to the patient name in the patients index data base (5), mentioned by the first institution (1a, 1b,? 1n).
7. System after one of the requirements 5 or 6, by the fact characterized that the central processing unit (4) the allocation of the produced alias to an institution (1a, 1b,? 1n) in the institutions index data base (6) stores.
8. System after one of the requirements 5 to 7, by the fact characterized that the central processing unit (4) the allocation of the produced alias to one in an institution (1a, 1b,? 1n) working person in the persons index data base (7) stores.

2 sheets designs follow

▲ top